TI - Method for making payments over mobile telephone system, comprises calculation of signatures during voice or data transmission using a mother key and diversified keys derived from the mother key

AB - FR2817108 NOVELTY - The user makes an order on the retailer WAP site which returns an offer (2) by SMS. The offer is validated by the user with a carrying code and the commercial details, signature and coded card number are returned (4) to the retailer. The retailer refers (5) the signature and coded card number to the bank who have the signature key and decoding means. On verification the bank informs the retailer (7) who signals (8) the user

- USE - To make payments over mobile telephone system
- ADVANTAGE - The system uses the SIM card installed in the mobile telephone to emit an electronic signature
- DESCRIPTION OF DRAWING(S) - The drawing shows the payment system.(The drawing includes non-English language text)
- Offer to user 2
- Return of data to retailer 4
- Refernce to bank 5
- Validation message from bank7
- Confirmation to user 8
- (Dwg.1/3)

PR - FR20000014826 20001117

PN - FR2817108 A1 20020524 DW200253 H04Q7/32 008pp

PA - (MERC-N) MERCURY TECHNOLOGIES SARL

IC - G06F17/60 ;H04Q7/32

IN - CREGO P

OPD - 2000-11-17

AN - 2002-492509 [53]

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 817 108**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 14826**

(51) Int Cl[7] : H 04 Q 7/32, G 06 F 17/60

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 17.11.00.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 24.05.02 Bulletin 02/21.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *MERCURY TECHNOLOGIES SARL* *Société à responsabilité limitée* — FR.

(72) Inventeur(s) : CREGO PIERRE.

(73) Titulaire(s) :

(74) Mandataire(s) :

(54) PAIEMENTS ELECTRONIQUES SUR LE RESEAU GSM/GPRS ET UMTS.

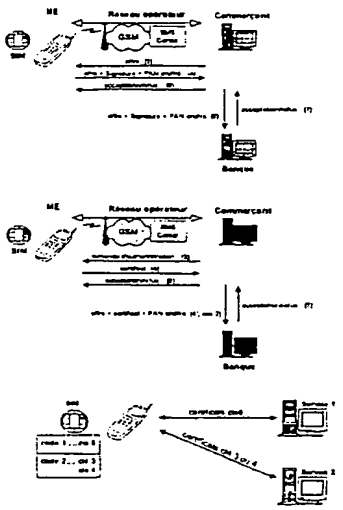
(57) La demande concerne un procédé de signature électronique et les applications (paiements) de ce procédé.

Le procédé de signature électronique selon l'invention met en oeuvre des réseaux de téléphonie mobile (23) de type GSM / GPRS et UMTS. On calcule des signatures à la volée, lors d'une session voix ou données, en utilisant, via un canal de signalisation (24) notamment un canal SMS, au moins une clé mère (21) et des clés diversifiées issues de ladite clé mère (22).

Ladite clé mère et lesdites clés diversifiés sont respectivement enregistrées:

. dans une zone mémoire (19) d'un serveur protégé (3) et

. dans une zone mémoire (19) de la carte SIM (11) d'un téléphone mobile (12). L'accès à ladite zone mémoire de la carte SIM étant contrôlé par un code d'identification personnel (13).



FR 2 817 108 - A1

3 Description des applications

Eléments constitutifs de l'offre*

Références numériques :

- Carte SIM =11
- Terminal Mobile ou poste client =12
- Serveur d'information WAP du commerçant =3
- Banque =9
- Bibliothèque de certification =14
- Applets sur carte SIM=15
- Usager ou client final=16
- Application=17
- Code personnel=18
- Zone mémoire du serveur de contrôle =19
- Zone mémoire de la carte SIM=20
- Clé mère =21
- Clé diversifiée=22
- Réseau de téléphonie mobile GSM/GPRS/UMTS=23
- Canal de signalisation SMS ou données =24

3.1 Paiements par transfert sécurisé du PAN (numéro de carte bancaire) (fig1)

3.1.1 Description

L'application de paiement est hébergée dans la carte SIM sous la forme d'une applet SIM Toolkit. Le paiement se déroule de la façon suivante :

1. Le client saisi sa commande sur le site WAP (3) du commerçant.
2. Le commerçant (3) envoie son offre par SMS.
3. L'offre (2) s'affiche sur le mobile du client (12) qui la valide par saisie d'un code porteur de paiement. Ce code n'est pas le PIN de sa carte SIM (11), et pas non plus celui de sa carte CB.
4. La transaction ainsi que le numéro de carte CB du client sont signés par une clé triple DES diversifiée. Le numéro de carte peut être saisi lors de l'opération, pré-saisi lors d'une phase de configuration de l'applet (15). Ce numéro de carte est de toute façon chiffré par cette même clé et l'ensemble des éléments de la transaction (4) (données commerçant, signature et numéro de carte chiffrés) sont retournés au commerçant (3).

4. Les éléments reçus sont signés par une clé triple DES et retournés au commerçant (3).
5. Si le commerçant (3) dispose de la clé de contrôle du certificat reçu (4) **cas n°1**), il peut assurer la réconciliation entre le certificat contrôlé correct et un numéro de carte CB (qu'il détient dans une base de données renseignée lors d'une procédure d'enregistrement préalable).

Si le commerçant (3) ne dispose pas de la clé de contrôle du certificat reçu (4) (ou s'il n'est pas autorisé à stocker des numéros CB **cas n°2**), il peut transférer l'ensemble des éléments reçus à une plate-forme bancaire qui réalisera la réconciliation avec un numéro CB.

6. La plate-forme qui détient la clé maître de l'application de paiement (commerçant (3) pour le cas 1, ou banque (9) pour le cas n° 2), contrôle le certificat (4) et opère une procédure standard de vente à distance basée sur le numéro de carte CB.
7. La plate-forme commerçant (3) (ou banque (9) via le commerçant (3)) signale au client (16) l'acceptation ou le refus de sa commande (8). La banque (9) indique au commerçant (3) son acceptation (tout était OK) ou son refus de la transaction (7), (la signature était fausse, le numéro de carte incorrect, ou les contrôles de risque refusés).

L'offre produit se compose

1. d'un ensemble de logiciels (**applets1 transfert du PAN et applets 2 authentification forte de l'usager**), adaptée à toutes les versions de carte SIM actives du marché
2. d'un ensemble de **bibliothèques de certification** utilisée par un serveur du commerçant ou de la banque permettant le dialogue par SMS avec l'applet.

Elles permettent :

- le calcul sur le téléphone mobile de certificats dynamiques (utilisables une seule fois, donc non re-jouables), après saisie par l'usager un code porteur applicatif,
- la modification des clés par des fonctions disponibles sur le mobile (fonction Over The Air)
- la modification par l'usager de son code porteur application.

3.3 Gestion des clés (fig 3)

La gestion des clés est un élément essentiel du système puisqu'elle permet le partage de l'applet entre plusieurs applications, tout en assurant l'étanchéité entre celles-ci.

3.4 Partage du système entre plusieurs applications

L'applet (5) gère jusqu'à 16 clés, identifiées par leur indice (0 à 15). Chaque clé appartient à une application, et chaque application gère un code porteur spécifique, différent du CHV1 demandé lors de la mise sous tension du mobile (2).

Exemple :

Application 1
Code porteur 1
Clé 0

Application 2
Code porteur 2
Clé 3
Clé 4

On peut alors gérer plusieurs applications simultanément comme l'accès à un paiement à distance (Application 1) et l'accès à un Intranet sécurisé (Application 2). L'usager saisit un code porteur différent selon le service auquel il accède, mais il a toujours la possibilité d'attribuer la même valeur à ses deux codes porteurs.

Revendications

Procédé de paiement électronique mettant en œuvre des réseaux de téléphonie mobile (23) de type GSM / GPRS et UMTS ; ledit procédé étant tel que :

- on calcule des signatures à la volée, lors d'une session voix ou données, en utilisant, via un canal de signalisation (14) notamment un canal SMS ou données, au moins une clé mère (21) et des clés diversifiées issues de ladite clé mère (22) ;

ladite clé mère et lesdites clés diversifiés étant respectivement enregistrées :

- dans une zone mémoire (19)d'un serveur protégé (3) et
- dans une zone mémoire (20) de la carte SIM (11) d'un téléphone mobile (12);

l'accès à ladite zone mémoire de la carte SIM (20) étant contrôlé par un code d'identification personnel (13).